

**POLICIES AND PROCEDURES  
OUACHITA TECHNICAL COLLEGE**

**SUBJECT AREA: Information Technology**

**POLICY/PROCEDURE: Minimum Standards for Networked Devices**

**DATE: 28 November 2006**

**NUMBER: 6.05**

**REVISION(S):**

**The following minimum standards are required for devices connected to the campus network.**

Software patch updates

Campus networked devices must run software for which security patches are made available in a timely fashion. They also must have all currently available security patches installed. Exceptions may be made for patches that compromise the usability of critical applications.

Anti-Virus software

Anti-virus software for any particular type of device currently listed on the Supported Software Policy (COPP 6.5) must be running and up-to-date on every level of device, including clients, file servers, mail servers, and other types of campus networked devices.

Passwords

Campus electronic communications systems or services must identify users and authorize access by means of passwords or other secure authentication processes. When passwords are used, they must meet the Minimum Password Complexity Standards (COPP 6.6). In addition, shared-access systems must enforce these standards whenever possible and appropriate and require that users change any pre-assigned passwords immediately upon initial access to the account.

All default passwords for access to network-accessible devices must be modified.

Where possible and appropriate:

- A. devices should be configured with separate accounts for privileged and unprivileged access;
- B. users should authenticate with an unprivileged account rather than a privileged account;
- C. privileged access should occur through a privilege escalation mechanism which allows the log to show which user was granted additional privileges;
- D. and privileged access should only be granted for as long as necessary to complete the task which requires additional privileges.

No unauthenticated email relays

Campus devices must not provide an active SMTP service that allows unauthorized third parties to relay email messages, i.e., to process an e-mail message where neither the sender nor the recipient is a local user.

Physical security

Unauthorized physical access to an unattended device can result in harmful or fraudulent modification of data, fraudulent email use, or any number of other potentially dangerous situations. In light of this, where possible and appropriate, devices must be configured to "lock" and require a user to re-authenticate if left unattended for more than 10 minutes.

Unnecessary services

If a service is not necessary for the intended purpose or operation of the device, that service shall not be running.

AUTHENTICATION (Signature):

COPP

\_\_\_\_\_  
President

28 November, 2006  
(Date)

**6.05**